FINAL

Operations Risk Management: Managing Your Integration and Test Risk[1]

James M. Lumsden, CSP
Jet Propulsion Laboratory
4800 Oak Grove Dr.
Pasadena, CA 91109
818-354-5667
james.m.lumsden@jpl.nasa.gov

Abstract—The risk of damage to program hardware during assembly, integration, and test activities prior to a project's "operational" phase is significant. Traditional Test Readiness Reviews are rarely sufficiently detailed to ensure that all aspects of a pending activity are appropriately addressed. A flexible, structured process that brings together appropriate disciplines to assess an impending activity has been developed and has been repeatedly shown to be value added.

The safety world is an intimate member of the overall Risk Management world, but is often perceived as overburdening projects with a plethora of rigid and highly specialized analyses. There is a need for analyses that have more flexibility and adaptability to be effective.

The survey process described here does all of this. It is a major tool in the overall Risk Management arsenal.

TABLE OF CONTENTS

1. INTRODUCTION

Systems Safety is an essential part of the entire team devoted to managing risk. While many organizations view the role of Systems Safety as limited to the safe design of a product, the role is most beneficial and cost effective when integrated with the product life cycle from concept to completion. This paper discusses the role of Systems Safety, and then describe a tool developed by JPL Systems Safety for effective utilization during the assembly, integration, and test phases of a project. The tool can also be used effectively during its operational phase.

Systems Safety as part of Risk Management

Systems Safety personnel take a 'system' level view of situations and configurations with the potential to injure personnel or damage hardware. This 'system' view can be done at any level of hardware assembly, from component level up to the entire system and beyond.

Risk comes in many colors and intensities. Different types of risk are best addressed by persons with capabilities to intelligently identify, and then assess, risks from many sources. Systems Safety personnel understand things that can "go wrong" and allow a system to get out of control, and can make suggestions to ensure involvement of the appropriate experts.

Systems Safety, like many Risk Management specialties, is often viewed as overburdening projects with a plethora of rigidized, highly specialized analyses. In reality, a good Systems Safety program is tailored to the needs and the risk tolerance of a particular project, and works as a part of the total team. It is tailored within a project to the risk tolerance at each level of assembly, from low level assemblies to the full system, and also tailored based on the particular point in the project's life cycle. Dependent on the risk tolerance of the project, an incident that damages hardware early in the life cycle inflict hardship, whereas an incident close to hardware or system delivery is potentially catastrophic for the project. The criticality of any incident is totally dependent on the project's risk tolerance.

Initial assessment of hazards in the system AND how they are controlled

The Systems Safety assessment process begins with a Preliminary Hazard Analysis (PHA), which identifies specific types of hazards and where they are located within the system. Once hazards are identified, intelligent decisions can be made to control the hazard to prevent the undesirable release of the controlled energy. The PHA is

[1] 0-7803-6599-2/01/$10.00 © IEEE

the backbone of any hazard analysis process because it starts with a system level view. More detailed analyses will be performed later in the detailed systems safety analysis, but for this discussion the PHA is fundamental.

Safety Survey Process

Testing is the backbone of any mission success program. It is almost always more preferable to test something than to rely on alternate means of verification. While all three methods have their pitfalls, most people have higher confidence in a test performed under the right conditions rather than rely on inspection and/or analysis. The principle of "Test what you fly: Fly what you test" means two things: first, flight hardware will be exposed to handling and testing environments throughout its prelaunch assembly, integration, and test phases; and second, the activities will include hazards which could jeopardize personnel safety. All of these activities must be closely scrutinized to ensure safety of personnel and the test hardware. The Safety Survey process described later in Section [3] was developed as a very beneficial and cost effective method to focus on safety of personnel and hardware. It involves personnel responsible for the safe conduct of an activity, as well as a Systems Safety Engineer who facilitates the process.

2. SYSTEMS SAFETY

What is Systems Safety?

System Safety is, "A systematic approach to the application of systems engineering and systems management to the process of hazard, safety and risk analysis to identify, assess and control associated hazards while designing or modifying systems, products, or services." In addition, "Before production, construction or operation, accident potential is eliminated or reduced by eliminating or controlling associated hazards. The system safety profession draws from a broad range of engineering, behavioral, scientific, legal and managerial skills."[2]

Every hazard must be controlled. The approach to be utilized in controlling any given hazard is a four step priority, beginning with the highest and most desirable approach:

1) Design the hazard out of the system;
2) Include hardware controls or inhibits to prevent the hazard from occurring;
3) Provide warning indications to allow human intervention; and/or
4) Procedural control.

The appropriate level or type of control, or combination of controls, must be assessed for each identified hazard based on the length of time the situation is present, the number of times an activity must be performed, and the consequences or severity of an accident actually happening. The controls must be carefully selected.

Occupational or Industrial safety is a vital part of the total System Safety team. They are the experts in specific areas of personnel safety and protection, and they keep abreast of all of the federal and state level Occupational Safety and Health Administration (OSHA) regulations and requirements. It is imperative that the Systems Safety analyses and activities involve the appropriate discipline experts as part of the team addressing any particular activity.

Two principle approaches:

In most cases, the specific hazard is an integral necessity for the system and cannot be designed out. The approach, then, moves to the next most desirable approach which is to design controls into the system. The two primary and most desirable control techniques are "Design for minimum risk" and "Fault Tolerance."

Design for Minimum Risk—The first control technique, "Design for minimum risk," is accomplished with a combination of special manufacturing and engineering techniques. Certain systems, such as pressure systems and vessels, do not lend themselves to multiple or redundant controls, therefore, design factors of safety and inspection techniques are relied on. Factors of safety vary depending on the type of service, and the handling and protection controls expected during the life of the system. For instance, pressure vessels in commercial and consumer service are typically designed with a safety factor of at least three (3) or four (4) based on the maximum pressure the vessel will see during its lifetime. Pressure vessels designed for spacecraft typically utilize a design factor of safety of 1.5 or 2.0, much lower than that used for commercial applications. However, the handling and inspection procedures in place provide protection for the vessel/system.

Fault Tolerance—The second control technique, "Fault Tolerance," incorporates multiple independent controls to prevent the unwanted occurrence of a function. For example, in its simplest form to protect against an inadvertent pyrotechnic function, three independently controlled relays would be placed in series between the power source and a pyro device, each independently controlled to avoid common cause failures. Variations that reliably accomplish the same level are, of course, permitted.

[2] Systems Safety Society, http://www.system-safety.org

Depending on the configuration, one of the three relays may be located in the power return leg, instead of on the supply side. One or two of the 'relays' may be solid state devices. The point is that the equivalent level of reliability must be designed into the system, and analyzed and tested to demonstrate it.

All applications of the "Fault Tolerance" method on control of a particular hazardous function must be analyzed to ensure true independence of each control. Many safety critical concerns about control of hazards can be addressed by the use of redundancy. If one system fails, the backup can be brought on line, or is already on line ready to assume control. In mechanical systems, hazards are frequently controlled by redundant safety elements, such as multiple pressure relief valves to prevent a catastrophe even if one valve fails to open when it is supposed to. Similar techniques are used in electronic circuits to prevent over voltage, over current, over temperature, etc. Often a combination of techniques is used, as in many lithium battery designs where multiple protections are designed in, each activating in turn as a dangerous overcharge or excessive current condition is approached, to prevent a catastrophic event.

Computer Controlled systems

One significant aspect of the systems safety role is in the area of computer controlled systems. In both the systems being designed and built, and in the testing facilities to test them, we are experiencing significantly increased reliance on computer systems, not only in the area of data gathering, but also in control and monitoring. We are immeasurably more efficient because of these machines, but we are also more vulnerable than ever to computer control problems.

In this day and age of computer-controlled systems, it is very easy to fall into the trap of assuming that multiple computer commands indicates fault tolerance. In fact, computers often proceed erroneously and issue multiple commands based on successfully passing some initial state verification. Using the example of multiple series switches, a primitive circuit may have ten (10) switches wired in series to control a function. If a single operator (the computer) controls all 10 switches, then the operator will proceed to activate all 10 switches whenever s/he thinks they have received the command to proceed. Computers are wonderful things, and in reality they are making our lives safer. But they must be properly designed into the overall system architecture, and the overall system architecture must be adequately analyzed for safety. This analysis cannot be performed piecemeal. It must be an overall, integrated system-level assessment.

Safety must be built in from the beginning. That is true in the hardware design and in the software design. Frequently, the hardware people and the software people are not in intimate contact regarding what the software is expected to do and how the hardware really operates. Safeguards are frequently not designed into the software to ensure the computer is operating properly, and that the data upon which it is operating is valid.

There are many examples of major failures due to insufficient systems level analysis of the computer/software/hardware system. Here are four examples, just to illustrate the point.

1. TERRA Spacecraft Safing—An example of a computer operating on invalid data was when NASA's TERRA spacecraft, an earth orbiter, went into safe mode on the day of the vernal equinox, the southerly maximum of the seasonal sine wave ground track above the earth's equator. The computer had tried to calculate the arcsine of a number slightly more negative than –1, which is an illegal operation and leads to a calculation error. The spacecraft was in safe mode for a week before the error was corrected and the spacecraft resumed normal operations. One could argue that the software operated as it was supposed to by entering safe mode, but an entire mission could be lost if a problem occurred at a critical moment.

2. *Radiation Treatment Machine*—Another example of improper computer programming was a radiation treatment machine that actually killed a person. The machine could be used in either a low power mode for diagnostics, or in a high power mode for treatment. The software was written to assume the state of the machine based on the keyboard input commands of the operator, not on the actual state of the hardware. The operators eventually became fast enough on the keyboard that multiple commands could be keyed in faster than the software could configure the hardware. The display indicated the machine was in the diagnostic mode so the operator proceeded with the test, not realizing that the machine was actually in the high power treatment mode. One patient that received excessive radiation exposure eventually died. Of course, the software was corrected, and this problem has not reoccurred, but our exposure to hazards due to computer-controlled systems is increasing every day.

Debugging software is an asymptotic process...you never get to zero defects.

3. Computer Controlled Test Equipment—In the realm of critical hardware testing, the test equipment is increasingly becoming computer controlled. The testing system for the Cassini spacecraft static structural load testing tower is a classic example. In this system, multiple hydraulic rams are

configured to exert loads on the 20 foot tall spacecraft to verify the design strength of the overall spacecraft structure. A computer was employed to control the load each cylinder was to apply to the structure, with appropriate over test limits programmed into the software. The system was efficient, and provided much more precisely controlled and more evenly applied loads to the total structure. What had not been considered until Systems Safety assessed the system was an understanding of what would happen to the loads in the structure during a power failure when the cylinders begin to suddenly unload at the same time, but at varying rates due to their varying sizes. An Uninterruptible Power Supply (UPS) was quickly added to the system to reduce the risk of sudden power outage affecting the test system.

4. *Reuse of Software*—The European Space Agency (ESA) lost the first Ariane 5 because of software. In order to save money, the program decided to utilize the Ariane 4 software in the Ariane 5 without a rigorous verification program. The assumption was that the Ariane 5 would fly the same as the Ariane 4, and that software had flown many times. In reality, the ascent profile of the Ariane 5 was sufficiently different that the in-flight guidance parameters exceeded the software capability, tumbling the vehicle out of control.

The entire system must be looked at as an integrated entity, not just individual elements.

Overall Systems Safety in Project Life Cycle

Concept—Systems Safety, when involved at the conceptual stage, has the opportunity to influence the system design to minimize the impact of hazard controls. Very often, they can suggest alternative methods of hazard control which can greatly reduce the complexity of the system, as well as ensuring that hazards are adequately controlled. It is very difficult to add necessary controls later in the life cycle.

Development—The typical environment in which a system is developed is difficult. Money is always tight. The schedule must be met, and is almost always too short. The typical mentality is that, "It won't happen to me." "Lightning won't strike here." While the probability of a lightning strike killing someone is low, it is a definite probability. Differing sources list 40-300 deaths/yr in USA, with the 30 yr avg about 73/yr. We can't eliminate lightning, but can reduce risk of a strike killing someone. Even so, NASA received a lightning hit on Apollo 12 during it's launch ascent, then lost an unmanned Atlas many years later for the same reason.
One of the important focus areas of Systems Safety is Lessons Learned. It is amazing to observe the attitude change during a discussion regarding a specific concern when someone thinks a particular scenario for potential damage is far fetched and a story in which that exact, or very similar, scenario actually occurred is presented. Experience shows that "it can happen to you."

Operational—During a system's operational lifetime, ongoing programs to properly maintain safety features designed into a system impact the operating cost. While an excellent tool for making comparisons of like systems in similar situations, attempts to perform cost/benefit analyses frequently play a disastrous role by forcing safety experts to place probability numbers on very low probability events, and then justify the predicted likely and maximum consequences. Modern day Life Safety Codes, which define local building and fire codes, have evolved over decades and centuries, partly because of learning new things and disaster behaviors, but also because of the cost/benefit tradeoffs which economic interests force into the system. It is expensive to incorporate safety into systems, and no one wants to pay for systems to protect against unlikely or low probability occurrences. The project will usually tend to do the minimum necessary, but liability after the fact can easily negate any previous cost savings.

When are you vulnerable?

We've been discussing the system safety aspect of system design, but there is another extremely important aspect to the overall safety program of any project, and that is protection of personnel and hardware during the development phase, usually comprised of assembly, integration, and test. In the spacecraft business, transportation to the launch site and launch site operations are also an important part of the development phase. We will concentrate here on space flight systems, which are typically very low 'production' quantities, but the principles apply to all types of projects. High volume production lines receive a lot of safety scrutiny, but the common mantra for 'one-sies' and 'two-sies' changes. The prevailing methodology is to place the responsibility for safety of the hardware, and of personnel during hardware testing and processing, with the Cognizant or Responsible Engineer. This person clearly has the responsibility to "be safe," but his/her focus is necessarily diluted by other extremely important factors, such as schedule, cost, staffing, procedures, facility availability, etc. A member of the team must be tasked with the "safety focus." This person should have a Systems Safety background.

During the subsystem and system level assembly, integration, test, transportation, and launch preparation activities, the system is extremely vulnerable to damage. Systems safety has a definite role with the project team to assess this phase of the project life cycle and assure proper

precautions are being taken. Systems Safety is trained to assess the operational system from both a bottom up and a top down perspective, and has tools to do exactly that.

Value Added Aspects to Project Team

Systems Safety brings a broad background to the team with specific focus on personnel and hardware safety into the development process. The two primary aspects of their expertise is in pretest planning and review, and in oversight during the test/activity. The primary test team is understandably success oriented and tends to be very focused. Systems Safety is always asking, "What if?" They are standing back and looking at the whole picture.

Outside influences or interactions

Systems Safety personnel are also trained to observe for other situations which can impact sensitive hardware. For instance, some spaceflight science instruments operate in the ultraviolet spectrum and are very sensitive to hydrocarbon contamination. In situations like these, the proximity of a machine shop to an assembly or test area for the instrument could lead to sufficient levels of hydrocarbon vapors migrating through air conditioning systems to catastrophically degrade the instrument performance. Certain optics materials are hygroscopic and degrade substantially if exposed to high humidity. Vibration exciters may use a slider table or block with an oil bearing to achieve one or more of the three orthogonal axes of the equipment being vibration tested. Extra care must be taken to protect sensitive detectors and optics from hydrocarbon vapor. In many cases, a single molecular layer of hydrocarbon contamination is sufficient to degrade the performance unacceptably.

Risk Tolerance

The importance put on Safety is USUALLY determined by superiors and outside forces such as budget constraints. The consequences of incidents are perceived differently by each player in the activity. It is easy for management to establish a goal to be 100 percent safe. In reality, a balance is necessary based on Project risk tolerance. Fortunately, the application of OSHA regulations for personnel safety eliminates the temptation for excessive shortcuts in that area. But, in the area of hardware safety, it is easy to succumb to the belief that "It won't happen to me."

Systems Safety personnel are a value added part of the overall project team specifically to provide this overall high-level assessment. They cannot act alone, but rather work most effectively when working interactively with the entire team.

3. Safety Survey: A Major Tool for Operations Safety Risk Management

A user friendly tool that brings Systems Safety expertise into the arena is not time consuming yet contributes significantly to the safe processing of flight hardware has been developed and implemented by Systems Safety personnel at JPL for more than a decade. The remainder of this discussion will concentrate on that tool.

Background

JPL has developed a tool, in the form of checklists, that have aided in the assessment of facilities and operations involved in the processing of flight hardware. The checklists are called "Surveys" specifically to avoid their application in the "checklist mentality." They are also NOT audit checklists. They are a list of thought provoking items to promote thorough assessment of every aspect of an activity. They have been utilized for hundreds of interactive surveys on literally dozens of flight projects since their inception in 1987.

Prior to development of the checklists, Systems Safety assessment of flight hardware processing areas and testing, was accomplished primarily by reliance memory. Environmental Testing assessment relied on a primitive set of seven very basic questions. Different Systems Safety personnel surveying activities put the emphasis on whatever their specific expertise led them to focus on, frequently omitting other important aspects of the activities that did not come to mind at the time, or were outside their experience base. As it is when looking back on incidents, it is not certain whether the survey process would have prevented that specific incident, but it definitely would have led to better test preparation by the test team.

When the author began to perform these initial assessments as someone new to Systems Safety, he recognized the need for something that would ensure that all significant aspects were appropriately addressed, not just selective ones. While in the process of developing his own checklist, an incident occurred during a thermal vacuum test of a very expensive science instrument. In the course of the investigation, high level management at JPL determined that a checklist of things to cover in the pretest assessment would be required as part of the corrective action plan. Within minutes, the draft checklist already in development was presented to management, and has been a fundamental foundation of the hardware and personnel protection aspect of Systems Safety program at JPL.

Checklist Scope

As initially implemented, the Safety Survey process was separated into two distinct checklists. The first one, the Facility Safety Survey (FSS), focused specifically on the facility or laboratory that would be processing flight hardware, and was intended for application to those facilities which process multiple flight items for many projects. The second list, the Operations Safety Survey (OSS), focused on the operation that would take place within that facility and involved both the facility personnel and the flight hardware personnel specific to that project. Because there is some redundancy between the two separate checklists, a combined checklist recently has been created which folds both the FSS and the OSS into a single combined checklist. The combined checklist is primarily intended for assessing those activities which are more specific to a particular project, such as an environmental test at a contractor, or a specific hardware processing or testing laboratory, where multiple projects will not be processed or tested at that facility. The Combined survey checklist is included as Appendix A.

The survey checklist contains 73 thought provoking items to address from a wide variety of sources, incorporating decades of Lessons Learned. In addition, the survey includes a list of potential hazards to stimulate thinking about what hazards might be involved in the activity being assessed. The survey can be focused very wide for broad, generic activities such as spacecraft buildup and electronics integration, or it can be focused very narrow for a specific hazardous activity within the overall Assembly, Test, and Launch Operations (ATLO) or Integration & Test (I&T) activity. An example of a narrow focused activity might be a pyro firing test or a special open air RF transmission test where special personnel safety controls and assessments might be required.

The emphasis in the survey process includes both personnel safety and flight hardware safety. It includes areas of emphasis such as:

Facilities
Integration of Flight Hardware into the Facility
Operations / Activities within the Facility
Personnel
Personnel Protection
Hardware
Test Readiness
Documentation / procedures

Items on the checklist range from mundane to exoteric, yet nearly every item has a lessons learned story to emphasize its importance and relevance. It forces the people involved to make sure they have given thought to some of the simple things that frequently are overlooked, or thought to have been taken care of by someone else.

Participants

An important feature of the surveys is establishing a mandatory attendance list (by function). As a minimum, the attendees are:

Hardware Cognizant Engineer
Quality Assurance
Facility Manager or responsible facility operator
Systems Safety Engineer
Occupational Safety Representative (if personnel hazards present)

Beyond these mandatory attendees, additional attendees are always welcome and often encouraged to attend. Depending on the magnitude of the activity, additional attendees may be:

Mission Assurance Manager
Project Office Representative
Environmental Requirements Engineer
Personnel Safety Specialists

Implementation

The frequency of these safety surveys depends on the specific activity, but as a minimum they must be repeated annually for an on-going activity such as ATLO or I&T. On-going activities are generally defined as those that are relatively continuous in nature, and do not have gaps or downtimes exceeding three months. The scope of the overall activity is defined for the survey, and any additional activity which is outside that scope is individually surveyed.

For instance, it is common for an overall I&T activity to be relatively hazard free. In this case, the survey is valid for one year. A special test which may introduce a hazard above and beyond the normal spacecraft testing activity, such as a pyro firing to test an appendage release mechanism, would receive its own separate survey.

The process may sound onerous, but in reality it is not. Most survey meetings last for approximately one hour, sometimes one and one-half hours. A meeting for an extremely complex spacecraft level environmental test may last for four hours. This is time well spent!

Benefits

The benefits of these surveys are enormous. One of the unfortunate realities of the safety business is that it is very difficult to prove effectiveness unless you can point to an improving accident/incident record, but that is very hard to do when the incident rate is low to begin with. The best that

can be done is to relate the feelings of those who go through the process.

One cognizant hardware engineer was extremely reluctant to participate. His approach was to deliver the hardware to the environmental test organization, along with the test requirements, and come back later to pick up his hardware. He was essentially informed by his management that he had to attend the survey meeting. A number of questions came up and were resolved at the meeting. Afterwards he approached the author and remarked that he was glad he had participated — quite an admission for a proud flight hardware owner!

A major intention of the survey meeting is to promote communication among the team members and to set the tone for the ensuing test while ensuring that all involved personnel recognize that there is only one Test Conductor. A frequent remark during the meetings is, "You're going to do WHAT to my hardware?" It is very common for the cognizant engineer to meet and understand the Environmental Test Specialist or test equipment operator for the first time. The discussions often go beyond traditional safety related concerns, fostering an open forum to ensure all planning aspects have been considered.

The benefits are even more dramatic when working with contractors. One survey at a very large Southern California aerospace contractor started off with a very icy reception of the JPL team invading the contractor's facility. He was quite proud of the facility, and actually did have a very clean and well run environmental testing shop. Since JPL had imposed the survey, he reluctantly participated. About one-half way through the survey checklist, he asked if he could interrupt for a minute. He went on to state, very meaningfully, that, "This is the best process I've ever seen. Can we have a copy of the checklists to incorporate into their own processes?" JPL was happy to oblige!

Other significant benefits are building the team for a specific activity, and providing a structured approach to ensure total coverage of all aspects of the activity. The survey ensures a multi-disciplinary evaluation to help cover all bases and avoid unwanted surprises.

Key Features

There are two key features of the survey process that are essential:

1) Management approval of the completed survey is required; and
2) The process has a lot of built-in flexibility.

It has been demonstrated that attitudes change when management approval is required. The approval requirement leads to better fidelity of the process. Sometimes Managers want more stringent controls in place than Systems Safety may be willing to accept. At times, the local manager's risk tolerance is lower than the specific project may be willing to accept. Consistency in understanding the risk tolerance among all involved is enhanced, particularly in a matrix management organization such as JPL where ultimately more than one manager may be responsible if something goes wrong.

Flexibility is the key to any good process. Situations, risk tolerances, and consequences constantly change. The survey process allows for significant flexibility as long as the fundamental principles are observed. The goal is to ensure that all persons involved have communicated essential information, that all persons involved are knowledgeable and properly trained, and that all persons involved know what the plans are, and that the inherent risks are identified and are acceptable.

4. Conclusion

Systems Safety is an important member of your project team, and an equally important element of overall risk management for the project. In addition to the traditional involvement in the actual project design, Systems Safety can bring important benefits into the assembly, integration, and test arena. There are many analysis tools available for the assessment of individual aspects of a project, but the tool presented here brings several significant aspects of analysis and assessment in a single user-friendly tool or process. By involving the owners of the safety responsibility and necessary discipline experts based on the hazards present, a much higher fidelity assessment results with an absolute minimum investment.

5. Acronyms

ATLO	Assembly, Test, & Launch Operations
CSP	Certified Safety Professional
ESA	European Space Agency
FSS	Facility Safety Survey
I&T	Integration and Test
JPL	Jet Propulsion Laboratory
NASA	National Aeronautics and Space Agency
OSHA	Occupational Safety and Health Administration
OSS	Operations Safety Survey

PHA	Preliminary Hazard Analysis
UPS	Uninterruptible Power Supply
USA	United States of America

REFERENCES

[1] System Safety Society, P.O. Box 70, Unionville, VA 22567-0070

[2] The Statistical Assessment Service, 2100 L St. NW, Suite 300 Washington, DC http://www.stats.org/index.html

[3] Office of Climate, Water, & Weather Services, National Weather Service, 1325 East-West Highway, Silver Spring, MD 20910

Jim Lumsden is a Systems Safety Engineer in the Systems Safety Office at the Jet Propulsion Laboratory. He has worked with spacecraft rocket propulsion and other hazardous systems since 1958. He has worked on spacecraft that visited every planet in the solar system except Pluto. He was the Systems Safety Manager for the Cassini Project, currently on its way to orbit Saturn. He is a Certified Safety Professional. He has a BS from the University of LaVerne.

ACKNOWLEDGEMENTS

This work was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Additional acknowledgement and thanks goes to the staff of the JPL Systems Safety Office who, over the years, have contributed immensely to the current form and content of the Safety Surveys. Special recognition goes to Dennis Ross and Ron Welch, who participated in the effort to combine the original Facility Safety Survey and Operations Safety Survey into the Combined Facility/Operations Safety Survey included in this paper.

APPENDIX A

SAMPLE OF COMBINED FACILITY/OPERATIONS SAFETY SURVEY

COMBINED FACILITY / OPERATIONS SAFETY SURVEY

Project:	**Subsystem(s):**	**Date of Survey:**
Activity:		**Operation Start:**
Responsible Engineer (Activity & H/W):	**Primary contact:**	**Operation End/Duration:**
Facility Name:	**Facility Location:**	**Facility modified since last survey?:** ❑ Yes ❑ No **N/A**
Facility Mgr:	**Bldg/Room:**	
Facility Equipment:		
❑ **Team Survey** ❑ **Informal Survey** (see pg. 5 for definitions):	**Survey Facilitator:**	

This Safety Survey checklist is intended to ensure that all personnel and hardware safety aspects of an activity are addressed by appropriate responsible and knowledgeable persons in a structured and orderly manner. It does not take the place of an Occupational Safety Program, nor does it absolve any organization of their responsibility to assure themselves of a safe working environment. Contractors are welcome/encouraged to employ their own checklist or survey process providing that their process has been reviewed & approved for its equivalent scope and applicability to the specific contract for the planned activity.

This survey is intended to assess readiness for flight-critical hardware operations, such as assembly, inspection, test activities, or storage, and shall include the integrated facility/hardware hazard analysis relationship. The survey shall be conducted sufficiently in advance to allow for action item closure prior to the commencement of the activity, and annually thereafter until completion.

All items in this safety survey checklist shall be assessed by the Facility/Operations Safety Survey Team and marked "YES", "NO", or "N/A" (Not Applicable) as appropriate for the scope of the activity. Corrective action or acceptance rationale for items assessed as "NO" shall be documented on page 4 of this survey. Action Items will be defined and documented in section (K) of this survey, and verified by Quality Assurance to be closed out prior to start of the test or activity. This checklist includes areas of concern that should be addressed, but are not necessarily all requirements. Checklist items may be tailored by crossing out or modifying as appropriate to properly convey the intended context.

List hazardous procedures, materials, pressure, temperature, power, voltages, frequencies, etc., in use during this operation. Address disposal of hazardous wastes or by-products. If additional space is required, continue on attached sheet.

Hazard*	**List Material, Procedure, etc.**	**Quantity**		**Remarks: Identify pressure, voltage, temperature, RF frequency, etc.**
		Facility	**Operation**	
***Hazard Type**	1. – Toxic 2. – Corrosive 3. – Explosive 4. – Pyrophoric	5. – Electrical 6. – Pressure 7. – Thermal 8. – Collision	9. – Ionizing Radiation 10. – Non-ionizing radiation 11. – Contamination 12. – Acoustic	13. – Fire 14. – Suffocation 15. – Static Charge Producers 16. – Other

List effluent products and waste from operation (for both normal and abnormal conditions).

Material	**Quantity**	**Condition**	**Discharge Products**	**Means of Disposal**
		Normal		
		Abnormal		
		Normal		
		Abnormal		
		Normal		
		Abnormal		

COMBINED FACILITY / OPERATIONS SAFETY SURVEY

YES NO N/A

A. HARDWARE STATUS

[ ] [ ] Hardware intended for this processing or testing activity is considered critical for the following reason(s):

[ ] Hardware intended for airborne or space flight, flight spares, or qualification
[ ] Long lead-time component destined to be incorporated into project-vital support equipment
[ ] Special handling/test equipment essential to the flight system, subsystem, or components
[ ] Unique tooling or fabrication fixtures
[ ] Shipping or transportation containers or equipment for flight systems, GSE, and spares
[ ] Project requirement
[ ] Other (explain): _____

B. FACILITY

[ ] [ ] [ ] 1. Previous Safety Survey Completed: Date of last Survey: _____. By whom?_____ (Organization/function)
[ ] [ ] [ ] 2. All action items closed out from last survey.
[ ] [ ] [ ] 3. Floor space, head room, accessibility adequate. Egress doors adequately identified (exit signs), operational & unobstructed.
[ ] [ ] [ ] 4. Illumination adequate for clear visibility of operations, test article, exits and emergency signs.
[ ] [ ] [ ] 5. Emergency lighting provided and functional.
[ ] [ ] [ ] 6. Floor loading within acceptable limits for all facility operations and posted where necessary.
[ ] [ ] [ ] 7. Hazardous obstructions, uneven floors, other obstacles removed or otherwise safed, including overhead structures/fixtures.
[ ] [ ] [ ] 8. Equipment/cabinets which could be hazardous to personnel or impact critical hardware during an earthquake secured.
[ ] [ ] [ ] 9. All cabling properly routed and secured.
[ ] [ ] [ ] 10. Facility instrumentation adequate, in calibration and tested (ISO compliant).
[ ] [ ] [ ] 11. Facility data displays and alarms adequate to indicate in-and-out-of specification conditions.
[ ] [ ] [ ] 12. Venting systems adequately sized and appropriately isolated from one another (including vacuum chamber GN_2 vents).
[ ] [ ] [ ] 13. Smoke/fire, toxic vapor detectors and alarms appropriately located and functioning.
[ ] [ ] [ ] 14. Fire blocking in service trenches and feedthroughs in place and effective. Trenches secure from flooding.
[ ] [ ] [ ] 15. Fluid, pneumatic, mechanical, electrical, and instrumentation configuration documented, controlled and readily available.
[ ] [ ] [ ] 16. Appropriate facility preventive maintenance plan exists, and maintenance and documentation are current.

C. HANDLING AND LIFTING EQUIPMENT

[ ] [ ] [ ] 1. Cranes, hoists, slings, fixtures, dollies and other lifting equipment, currently certified and proof tested.
[ ] [ ] [ ] 2. Lifting equipment (slings, spreader bars, etc.) equipped with umbrella or shield for hardware protection (if req'd).
[ ] [ ] [ ] 3. Crane safety requirements posted on all crane control pendants.
[ ] [ ] [ ] 4. List of qualified crane operators posted and current.
[ ] [ ] [ ] 5. Lifting devices thoroughly inspected prior to use. (Pre-lift safety meeting required prior to any lifting operations).

D. CRITICAL HARDWARE PROTECTION MEASURES

[ ] [ ] [ ] 1. Suitable clean agent fire extinguishers available, and personnel briefed in proper selection and use (Cleanguard, CO_2, etc.).
[ ] [ ] [ ] 2. Hardware protected from overhead water systems (sprinklers deactivated or covers utilized, broken plumbing repaired etc.).
[ ] [ ] [ ] 3. ESD protection appropriate (garments, proper grounding, placards), and ESD survey completed, by Q.A., if required.
[ ] [ ] [ ] 4. Temperature/humidity control and monitoring systems in place and calibrated. Limits appropriate for specific hardware.
[ ] [ ] [ ] 5. Contamination controlled to appropriate levels (volatiles, particulates, food, beverages, smoking prohibited, etc.).
[ ] [ ] [ ] 6. Personnel access to test areas and equipment controlled to appropriate levels considering sensitivity/criticality of hardware.
[ ] [ ] [ ] 7. Buddy system in effect when critical hardware accessible or operating.
[ ] [ ] [ ] 8. Area secured and checked by security during nonworking hours and security informed when flight hardware present.
[ ] [ ] [ ] 9. Appropriate lightning, surge, overvoltage protection implemented. Facility ground verified. (Date _____)
[ ] [ ] [ ] 10. Full time operator coverage available during critical operations or transitions and when test article is powered.
[ ] [ ] [ ] 11. QA coverage in place during test set-up, hardware handling, pre-test/ post test operations, and critical transitions.
[ ] [ ] [ ] 12. Hardware stable/secured during all phases of testing and non-test conditions, including storage.
[ ] [ ] [ ] 13. Fire department notified and informed of special responses required for critical hardware.
[ ] [ ] [ ] 14. Facility/GSE/Flight Hardware system safe in power-off state (i.e: power <u>not</u> required to remain safe).
[ ] [ ] [ ] 15. Effects of power failures, loss of utilities (H_2O, gas/fuel, LN_2, GN_2, etc.), glitches, or transients understood and acceptable.
[ ] [ ] [ ] 16. GSE & facility designed to "fail-safe" for personnel and critical hardware.
[ ] [ ] [ ] 17. Backup facility and/or GSE electrical power (UPS) available if required for hardware protection and/or emergency situations. (UPS systems location & battery condition verified safe)
[ ] [ ] [ ] 18. Hazardous/flammable materials identified, minimized, properly contained, and disposal methods authorized.
[ ] [ ] [ ] 19. Space flight hardware signs posted in test areas, and on all flight hardware transport containers.
[ ] [ ] [ ] 20. At least one overtest protection device and sensor(s), independent of the automatic primary controller, closely coupled to the critical hardware, calibrated, and verified operational.
[ ] [ ] [ ] 21. Environmental facility and test fixture combination operated over specified environmental range and qualified prior to use with flight critical item.

COMBINED FACILITY / OPERATIONS SAFETY SURVEY

YES NO N/A

D. CRITICAL HARDWARE PROTECTION MEASURES (Cont'd)

[ ] [ ] [ ] 22. Adjacent activities which could impact critical hardware, GSE, or test activities controlled or eliminated.
[ ] [ ] [ ] 23. Operating personnel understand that, in case of anomaly, all actions must be toward returning to a safe condition for personnel and hardware. Anomaly and troubleshooting activities require approved procedures.
[ ] [ ] [ ] 24. Key test parameters (vital for flight hardware protection and verification) continuously and automatically recorded, and incorporated in shut-down circuit, if appropriate.
[ ] [ ] [ ] 25. GSE displays adequate to unambiguously indicate in-and-out-of-specification conditions.
[ ] [ ] [ ] 26. GSE & facility calibration/validation/proofing current (ISO Compliant).
[ ] [ ] [ ] 27. GSE & facility pressure/vacuum vessels/systems conform to code requirements, components properly labeled, restrained, relieved, and tested/validated.
[ ] [ ] [ ] 28. Electrical configurations conform to code requirements, properly labeled, protected, isolated, fused, and insulated.

E. FACILITY AND HARDWARE PERSONNEL PROTECTION

[ ] [ ] [ ] 1. Personnel location during test or activity is safe.
[ ] [ ] [ ] 2. All facility and hardware personnel involved briefed on test objectives/conduct/procedures.
[ ] [ ] [ ] 3. Qualified and familiar with normal facility and test hardware operation and with emergency test response and operation, including power, water, communication, heating/cooling, gas/fuel, LN_2, or other utility failure responses.
[ ] [ ] [ ] 4. Trained and qualified for specific hazardous operations, planned & contingency (lasers, radiation, hazardous materials, etc).
[ ] [ ] [ ] 5. Specific personnel responsibilities and chain of command documented and understood. Test Director designated.
[ ] [ ] [ ] 6. Sufficient qualified personnel available to avoid overload or fatigue during test operations.
[ ] [ ] [ ] 7. Briefed on facility alarms, basic emergency responses, etc.
[ ] [ ] [ ] 8. Communications properly coordinated and tested (test conductor, facility & hardware test personnel, emergency, etc.).
[ ] [ ] [ ] 9. Emergency communication services appropriate and readied, including fire and security departments. Emergency vehicle access adequate.
[ ] [ ] [ ] 10. Emergency phone list of critical test personnel conspicuously posted in test area. Copy provided to security for approved unattended operations. (Note: List facility analog phones since digital phones are non-operable during power cuts)
[ ] [ ] [ ] 11. Personnel Protective Equipment (PPE) available for planned or emergency use. Personnel trained in use. (Low O_2, emergency breathing, toxic vapor warning and protection. etc).
[ ] [ ] [ ] 12. Personnel conducting hazardous operations included in a medical surveillance program.
[ ] [ ] [ ] 13. Warning placards and shielding against hazardous environments, explosives, flammables, toxic vapors, oxygen depletion, high pressures, temperatures, voltages, cryogenics, radiation (ionizing or non-ionizing, laser), sonic or audio levels, unattended operating equipment.
[ ] [ ] [ ] 14. Live mechanical/electrical parts suitably guarded (belts, vents, gauges, rotating machinery, Ground Fault Circuit Interrupters, etc.).
[ ] [ ] [ ] 15. Material Safety Data Sheets (MSDS) current and readily available for all hazardous materials in activity (Facility & Operation).

F. TEST DOCUMENTATION

[ ] [ ] [ ] 1. Approved written detailed test procedure(s) for operation of the facility for this specific activity, including approved test levels and specific facility/test item interactions.
[ ] [ ] [ ] 2. Transportation, lifting/handling procedure completed and approved. Identified as HAZARDOUS or NONHAZARDOUS with appropriate CAUTION and WARNING notations.
[ ] [ ] [ ] 3. Approved written hardware functional test procedures, dry run (if appropriate).
[ ] [ ] [ ] 4. Flight hardware/test item and GSE configuration documented and photographed.
[ ] [ ] [ ] 5. Specific environments and test levels approved by Environmental Requirements.
[ ] [ ] [ ] 6. Emergency plan and procedures, if necessary, covering contingencies (exclusive of facility considerations) for events such as earthquake, fire, loss of power or consumables, spillage, etc.

G. ANALYSES

[ ] [ ] [ ] 1. Integrated hardware/facility hazard analysis or fault tree calculated to sufficient level and formality to assure personnel, facility and hardware safety (Note: This survey <u>may</u> suffice in most cases).
[ ] [ ] [ ] 2. Previous problems/failures resolved to prevent recurrence.

H. BRAIN TICKLER

Other items which could possibly affect personnel, hardware, or facility safety. Please record these items:

[ ] [ ] 1. _____

[ ] [ ] 2. _____

COMBINED FACILITY / OPERATIONS SAFETY SURVEY

I. LIST OF ATTENDEES:

NAME	ORG	FUNCTION	email

J. RATIONALE FOR ACCEPTING "NO" ANSWERS:

LINE ITEM	RATIONALE

K. ACTION ITEMS (To be verified by QA as CLOSED or COMPLETED prior to test initiation):

AI#	LINE ITEM	ACTION	RESPONSIBILITY

SIGNATURES:

Facility Section Manager Date

Hardware Cognizant Secton Manager Date

COMBINED FACILITY / OPERATIONS SAFETY SURVEY

APPLICABILITY

	Assy	Storage	Insp	Funct Test (Non-Env)	Funct Test (Env)	Env Qual, PF, FA
System	T	T	T	T	T	T
Subsystem	T	T	T	T	T	T
Assy	I	I	I	T	T	T
Subassy	I	I	I	I	T	T
Comp	I	I	I	I	I	I

Facilities and operations involving flight-critical hardware require a Safety Survey: The choice of Team (T) Survey or Informal (I) Survey is determined by the nature of the operations and the level of assembly of the hardware. Flight-critical hardware is defined as hardware whose loss or damage would significantly impact the Project in either cost or schedule, as determined by the hardware Contractor and/or Project.

T = Team Survey:

Requires completion of a Contractor Facility/Operations Safety Survey by the Facility Manager and/or Hardware Cognizant Engineer and review by a survey team comprised of: (1) the Hardware Cognizant Engineer, (2) the Facility Manager, (3) a Systems Safety Office Representative, (4) an Occupational Safety Office Representative (if personnel hazards are involved in the operation), (5) an Environmental Test Laboratory Representative (if environmental testing is involved), and (6) the Quality Assurance Representative. Additional key Project Office personnel shall be notified and given the option of attending.

Items assessed as NO during the survey must be dispositioned by the Team (accepted or referred to a higher authority) prior to the operation. Completion of the Team Survey constitutes consent to proceed pending QA verification of action item closure prior to the activity (or within 30 days if the activity is a continuing activity) or as stated in the minutes.

NOTE: If a formal Test Readiness Review is conducted, the results of this survey should be reported at that review.

I = Informal Survey:

Necessitates the completion of a Safety Survey by the Facility and/or Operation Manager prior to the operation. Action items and all items assessed as NO or N/A should be reviewed by the appropriate Manager for concurrence. Action items may remain open with approval of the appropriate Manager, but must be closed prior to any activity requiring a higher level of review.

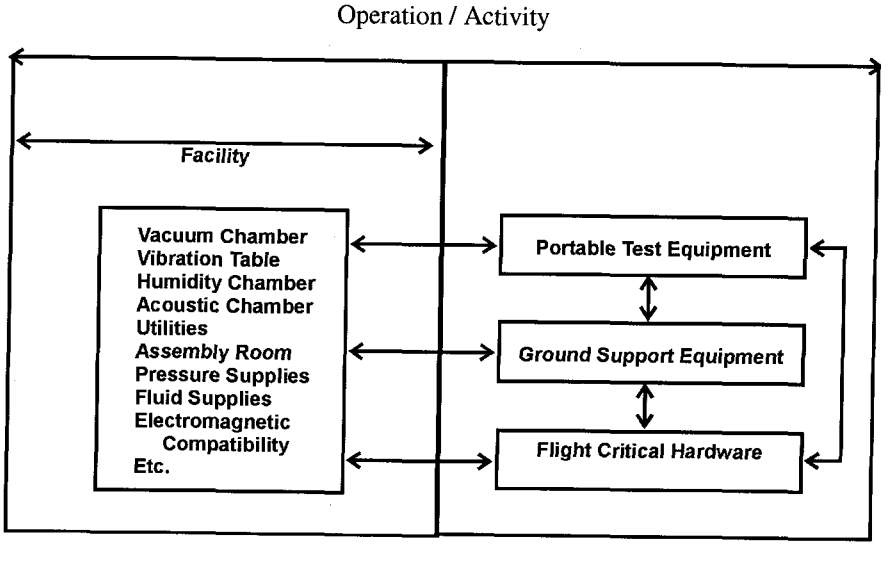

Figure 1: Relationship of Facility to Operation